ABSTRACT OF THE DISCLOSURE

A thin client VPN capable end system reduces the vulnerability of corporate networks to malicious code introduced by remote workers. The end system is denied network connectivity except for conducting VPN sessions. The end system is made virtually impervious to permanent infection by directing all data writes during VPN sessions to a temporary memory that is purged at the end of the session. Thus, the end system cannot acquire malicious code in personal sessions and the corporate network administrator can eradicate any malicious code acquired by the end system in a VPN session by shutting down the VPN and cleaning up the corporate network.